S

HP OpenView for Windows User Guide
“HP OpenView”

HP OpenView and the Internet standards invalidate the indicated claims under 35 U.S.C. § 102(b) and 35 U.S.C. § 103*

All text citations are taken from:

- HP OpenView for Windows User Guide for Transcend Management Software, Version 6.1 for Windows and ’97 for Windows NT, 3Com, October 1997 (hereinafter “HP OpenView for Windows User Guide”) [SYM_P_0080944- SYM_P_0081098].
- RFC 1157, A Simple Network Management Protocol (SNMP), May 1990 [SYM_P_0501113- SYM_P_0501142] and [SYM_P_0527111]
- RFC 1155, Structure and Identification of Management Information for TCP/IP-based Internets, May 1990 [SYM_P_0501012- SYM_P_0501031].
- RFC 1213, Management Information Base for Network Management of TCP/IP-based internets: MIB-II, March 1991 [SYM P 0501143- SYM P 0501205].
- RFC 1271, Remote Network Monitoring Management Information Base, November 1991 [SYM_P_0501206- SYM_P_0501271].
- RFC 2021, Remote Network Monitoring Management Information Base Version 2 using SMIv2 , January 1997 [SYM_P_0603708- SYM_P_0603837]

The text included herein are merely representative samples of the disclosure in the asserted reference. I reserve the right to supplement these disclosures.

<u>102(b)</u>

HP OpenView for Windows User Guide and RFCs 1155, 1157, 1213 and 1271 constitute a single disclosure for purposes of 35 USC § 102(b) because HP OpenView for Windows User Guide incorporates-by-reference the text of these RFCs. HP OpenView for Windows User Guide devotes several chapters to the use of SNMP: *see, e.g.*, Chap. 5 “Managing SNMP Network Devices,” and Chap. 7 “Custom Controls.” HP OpenView for Windows User Guide specifically references and relies upon the information in these RFCs:

* 103 references are identified under the heading “**<u>103:</u>**”.

HP OpenView for Windows User Guide
"HP OpenView"

"The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB).... The SNMP Manager supports all Internet MIB-II variables and can be extended to support other MIBs." (5-1) [SYM_P_0081033].

"MIB-2 dependent MIBs, such as rmon, would be added to the structure under the MIB-2 group" (5-19) [SYM_P_0081051].

"OpenView provides the MIBs for both MIB-2 (RFC1213) and rmon (RFC1271)." (5-20) [SYM_P_0081052].

103

In the alternative, HP OpenView for Windows User Guide in combination with RFCs 1155, 1157, 1213 and 1271 renders the patents invalid due to obviousness under 35 USC § 103. The citations above provide a motivation to combine in order to make and improve the network traffic monitoring claimed in the patents-in-suit.

Similar disclosures and additional related information are contained in the following additional references:

- HP OpenView for Windows Workgroup Node Manager User Guide, Transcend Management Software version 6.0 for Windows, 3Com, January 1997 [SYM_P_0081099-SYM_P_0081212].
- M. Siegl, and G. Trausmuth, "Hierarchical Network Management – A Concept and its Prototype in SNMPv2," 1996 [SYM_P_0500982- SYM_P_0500991].
- HP SNMP/XL User's Guide, HP 3000 MPE/iX Computer Systems Edition 5, Hewlett Packard, April 1994 [SYM_P_0076931- SYM_P_0077019].
- RFC 1441, Introduction to version 2 of the Internet-standard Network Management Framework, April 1993 [SYM_P_0501272- SYM_P_0501284].
- RFC 1757, Remote Network Management Information Base, February 1995 [SYM_P_0501319- SYM_P_0501399].
- RFC 1451, Manager-to-Manager Management Information Base, April 1993 [SYM_P_0501285- SYM_P_0501318].
- Mark Miller, Managing Internetworks with SNMP, Second Edition, 1997 [SYM_P_0503966- SYM_P_0504693].

HP OpenView for Windows User Guide
“HP OpenView”

‘203 Claim number	Claim Term	HP OpenView (printed publication and public use)
1	A computer-automated method of hierarchical event monitoring and analysis within an enterprise network comprising:	The HP OpenView Workgroup Node Manager is a “platform” for network management programs. It provides a standard graphic “interface so that multiple network applications can share a common display and alarm system. In addition, it provides basic network management functions to interface with devices on the network.” (1-1) [SYM_P_0080957] “Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.” (RFC 1157 p 4) [SYM_P_0527111]
	deploying a plurality of network monitors in the enterprise network;	“Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background.” (1-2) [SYM_P_0080958] “**Trapping** Some devices can send messages when certain conditions occur. The conditions may be startup, shutdown, data error, or a preset level of activity. The message resulting from a device condition is called a trap. … Once devices are configured to send traps to the OpenView console, they will be recorded in the alarm log by default. You can customize how OpenView responds to traps using the Customize Traps dialog. You can select which traps to respond to. The traps can be of particular types or from particular device classes. … When OpenView receives a trap message OpenView converts it into an alarm and processes it through the alarm system.” (1-5) [SYM_P_0080961] “Other symbols in the Compound Object category are used for devices that provide internal configuration information to OpenView.

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		If a supporting application is installed, opening one of these could display hardware configuration and status, memory usage, disc space, or installed software…. The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996] "One of the keys to using the SNMP Manager is understanding the structure of the MIBs. … MIB-2 dependent MIBs, such as **rmon**, would be added to the structure under the MIB-2 group." (5-19) [SYM_P_0081051] --------------------------------- "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices … An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208] "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements." (RFC 1157 p 4) [SYM_P_0527111] "The SNMP models all management agent functions as alterations or inspections of variables. Thus, a protocol entity on a logically remote host (possibly the network element itself) interacts with the management agent resident on the network element in order to retrieve (get) or alter (set) variables. … The strategy implicit in the SNMP is that the monitoring of network state at any significant level of detail is accomplished primarily by polling for appropriate information on the part of the monitoring center(s). A limited number of unsolicited messages (traps) guide the timing and focus of the polling." (RFC 1157 p. 6) [SYM_P_0501115]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
	detecting, by the network monitors, suspicious network activity	**"Configuring Alarms** Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following: … Forward an alarm to another management console Sound an alarm" (4-21) [SYM_P_0081019] "Critical alarms are grouped before warning alarms. and alarms within status groups are displayed in chronological order." (4-23) [SYM_P_0081021] "The OpenView SNMP custom controls provide visual indications of the values of SNMP variables for any SNMP device. .. The controls also have an Alarm capability which allows you to set low and high thresholds which will cause the control to change from normal to alarm colors when those thresholds are exceeded." (7-1) [SYM_P_0081059] "MaxThreshold Defines the upper limit for this variable. If the variable exceeds this value, and there is not an outstanding alarm condition, an alarm event will be generated and the control will be displayed in AlarmColor if Alarm=Max/Min Thresholds. If the Trap property is set to TRUE an OpenView alarm will be sent to the AlarmManager." (7-6) [SYM_P_0081064] "MinReset Defines the value that the variable must reach, after crossing the threshold, to reset the alarm condition." (7-7) [SYM_P_0081065] "MinThreshold Defines the lower limit for the variable. If the variable drops below this value, and there is not an outstanding alarm condition, an alarm event will be generated and the control will be displayed in AlarmColor if Alarm=Max/Min Thresholds. If the Trap property is set to TRUE an OpenView Alarm will be sent to the AlarmManager." (7-7) [SYM_P_0081065]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Trap Trap is used to tell the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared… If set to True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. These traps will result in alarms in the OpenView Alarm Log." (7-8) [SYM_P_0081066] "**Trap** – tells the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared. If False (default) no SNMP Traps will be sent. If True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. … One of the methods to indicate alarms is to determine a *normal operating range* for a particular variable." (7-11) [SYM_P_0081069] "Many variables do not fit into the standard threshold definition. For example, a port on an Ethernet hub might have a variable that represents 'link status' … To provide support for these variables, another form of thresholds has been provided with two additional properties. These properties are **NormalValues** and **AlarmValues**." (7-12) [SYM_P_0081070] ---" • Problem Detection and Reporting The monitor can be configured to recognize conditions, most notably error conditions, and continuously to check for them. When one of these conditions occurs, the event may be logged, and management stations may be notified in a number of ways. • Value Added Data Because a remote monitoring device represents a network resource dedicated exclusively to network management functions, and because it is located directly on the monitored portion of the network, the remote network monitoring device has the opportunity to add significant value to the data it collects. For instance, by highlighting those hosts on the network that generate the most traffic or errors, the probe can give the management station precisely the information it needs to solve a class of problems." (RFC 1271 p. 3-4) [SYM_P_0501208- SYM_P_0501209]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"The Event group controls the generation and notification of events from this device. Each entry in the eventTable describes the parameters of the event that can be triggered. Each event entry is fired by an associated condition located elsewhere in the MIB. An event entry may also be associated with a function elsewhere in the MIB that will be executed when the event is generated. For example, a channel may be turned on or off by the firing of an event. Each eventEntry may optionally specify that a log entry be created on its behalf whenever the event occurs. Each entry may also specify that notification should occur by way of SNMP trap messages. In this case, the community for the trap message is given in the associated eventCommunity object. The enterprise and specific trap fields of the trap are determined by the condition that triggered the event. Three traps are defined in a companion document: risingAlarm, fallingAlarm, and packetMatch." (RFC 1271 p. 67) [SYM_P_0501267]
	based on analysis of network traffic data selected from the following categories: {network packet data transfer commands, network packet data transfer errors, network packet data volume, network connection requests, network connection denials, error codes included in a network packet};	"The Simple Network Management Protocol (SNMP) Version 1 is a standard that defines a method of communicating with and controlling network devices. Devices that support SNMP V.1 standard can be queried for their status and other device information. … OpenView provides an SNMP Management function that can be used to communicate with SNMP devices. The device settings and other device information are available as variables and are defined either in a standard Management Information Base (MIB) file or in a custom MIB file proved by the device manufacturer." (1-7) [SYM_P_0080963] "**DataType** – can be set to Absolute or Delta. This tells the control whether to display the actual value that was returned from the SNMP device (Absolute) or the difference in the variable since the last poll (Delta). The Text Box control could be used to poll the UDPInDatagrams of a device. If you set the DataType of the control to Absolute, you will see a constantly incrementing value displayed which is the total since the last delivery reset. If you set DataType to Delta, you will see a number that represents the number of UDPInDatagrams since the last poll." (7-10) [SYM_P_0081068] -- "ifInUnknownProtos OBJECT-TYPE … DESCRIPTION 'The number of packets received via the interface which were discarded because of an unknown or unsupported protocol.'" (RFC 1213 p. 19) [SYM_P_0501161]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"ifOutErrors OBJECT-TYPE … DESCRIPTION 'The number of outbound packets that could not be transmitted because of errors.'" (RFC 1213 p. 20) [SYM_P_0501162] "ipInHdrErrors OBJECT-TYPE… DESCRIPTION 'The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, etc.'" (RFC 1213 p. 24) [SYM_P_0501166] "icmpInErrors OBJECT-TYPE … DESCRIPTION 'The number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.)'" (RFC 1213 p. 36-37) [SYM_P_0501178- SYM_P_0501179 "tcpActiveOpens OBJECT-TYPE … DESCRIPTION 'The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.'" (RFC 1213 p. 42) [SYM_P_0501184] "tcpPassiveOpens OBJECT-TYPE… DESCRIPTION 'The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.'" (RFC 1213 p. 42) [SYM_P_0501184] "tcpAttemptFails OBJECT-TYPE … DESCRIPTION 'The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.'" (RFC 1213 p. 42-43) [SYM_P_05001184- SYM_P_0501185]

HP OpenView for Windows User Guide
“HP OpenView”

‘203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		“tcpOutRsts OBJECT-TYPE … DESCRIPTION ‘The number of TCP segments sent containing the RST flag.’” (RFC 1213 p. 46) [SYM_P_0501188] “etherStatsOctets OBJECT-TYPE … DESCRIPTION ‘The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including FCS octents).’” (RFC 1271 p. 13) [SYM_P_0501218] “etherStatsPkts OBJECT-TYPE … DESCRIPTION ‘The total number of packets (including error packets) received.’” (RFC 1271 p. 13) [SYM_P_0501218] “The Alarm group periodically takes statistical samples from variables in the probe and compares them to thresholds that have been configured.” (RFC 1271 p. 24) [SYM_P_0501229] See table of SNMP/RMON in my expert report.
	generating, by the monitors, reports of said suspicious activity; and	“Some devices can send messages when certain conditions occur. The conditions may be startup, shutdown, data error, or a preset level of activity. The message resulting from a device condition is called a trap. … Once devices are configured to send traps to the OpenView console, they will be recorded in the alarm log by default. You can customize how Openview responds to traps using the Customize Traps dialog. You can select which trap to respond to. … When OpenView receives a trap message OpenView converts it into an alarm and processes it through the alarm system.” (1-5) [SYM_P_0080961] **“Applications and Alarms** Equipment manufacturers create application programs to provide information on the status of their devices. Application programs can request status information from the device, make device settings, or run device diagnostics. The application program then sends the appropriate information to OpenView as alarms.” (1-6) [SYM_P_0080962]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Monitoring Traps from Network Devices Traps are specific types of messages that are generated by some devices to indicate a change in their status. When a device is installed on the network part of its installation procedure is to enter the address of a management console where these traps are to be sent. Refer to the device installation and configuration documentation and set the trap address to the network address of the OpenView console." (4-10) [SYM_P_0081008] "Trap is used to tell the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared... If set to True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. These traps will result in alarms in the OpenView Alarm Log." (7-8) [SYM_P_0081066] "**Trap** – tells the control whether to send an SNMP Trap packet whenever alarm conditions are set or cleared. If False (default) no SNMP Traps will be sent. If True, SNMP Traps will be sent to OpenView whenever a threshold is crossed that creates an alarm condition, and also whenever a reset value is crossed causing an alarm condition to be cleared. … One of the methods to indicate alarms is to determine a **normal operating range** for a particular variable." (7-11) [SYM_P_0081069] "The Simple Network Management Protocol (SNMP) Version 1 is a standard that defines a method of communicating with and controlling network devices. Devices that support SNMP V.1 standard can be queried for their status and other device information." (1-7). [SYM_P_0080963]
	automatically receiving and integrating the reports of suspicious activity, by one or more hierarchical monitors.	"Once devices are configured to send traps to the OpenView console, they will be recorded in the alarm log by default. You can customize how Openview responds to traps using the Customize Traps dialog. You can select which trap to respond to. … When OpenView receives a trap message OpenView converts it into an alarm and processes it through the alarm system." (1-5) [SYM_P_0080961] **"Alarms**

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		Changes in device status or "alarms" provide the notification to the OpenView map that a noteworthy event has happened on the network. Alarms are the main mechanism used to communicate device status. Alarms are displayed on the network map and are listed in the Alarm Log. The alarms are also recorded in a Paradox database. The Alarm database allows you to generate reports or archive network performance. In addition to visual cues, alarms can be set to trigger sounds, programs, or even activate a remote paging device based on the type of alarm received." (1-3) [SYM_P_0080959] **"Alarm System** OpenView allows you to configure how alarms will be processed or displayed on maps, clear alarm conditions, and create reports from the alarm log. In addition, you can configure alarms of a particular level to start programs, send pages, or be forwarded to other workstations." (1-6) [SYM_P_0080962] "The submap symbol displays the most severe status color for all of the nodes or devices within it. This allows the most severe status information for any device in the network to be propagated up to the home submap. The home submap can then give you an overview of status for the entire network." (3-2) [SYM_P_0080984] "OpenView provides several different ways that you can monitor the devices in your network. You can: … Monitor trap messages sent by network devices alerting you to changes in device status. Configure how alarms are processed, displayed, recorded, and forwarded." (4-1) [SYM_P_0080999] **"Automatically Acknowledging Alarms Generated by Traps** The Acknowledge on Matching Trap and Variable text box allows you to clear a trap when a new specified trap is received. The original trap is moved from the current alarm log to the history alarm log. A variable in the trap packed that holds the network object's name can be selected to match the subobject field in the alarm log. This is to make sure that a trap that clears an alarm is referring to a particular device." (4-16) [SYM_P_0081014]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Managing Alarms Alarms generated by applications, traps, or polling are managed through the map, alarm log, and alarm forwarding functions." (4-17) [SYM_P_0081015] **"Status Propagation** You can select the way device status is propagated to higher submap levels using **Customize Alarms** in the **Options** menu. Status propagation can be set to: Do not pass status up Pass status up one level Pass status up all levels" (4-18) [SYM_P_0081016] "**Frequency** – this setting is used to prevent multiple alarms of the same state from the same device. Duplicate alarms will be ignored if they occur within the specified time period." (4-26) [SYM_P_0081024] "Alarms can be forwarded to another console. This is useful in complex networks where there is a hierarchical network management scheme using multiple consoles. A console monitoring a local network can pass status information on devices in its network to a master console. Selected alarms at the local console can be converted to traps and sent to another console." (4-28) [SYM_P_0081026]
2	The method of claim 1, wherein integrating comprises correlating intrusion reports reflecting underlying commonalities.	**"Automatically Acknowledging Alarms Generated by Traps** The Acknowledge on Matching Trap and Variable text box allows you to clear a trap when a new specified trap is received. The original trap is moved from the current alarm log to the history alarm log. A variable in the trap packed that holds the network object's name can be selected to match the subobject field in the alarm log. This is to make sure that a trap that clears an alarm is referring to a particular device." (4-16) [SYM_P_0081014] "**Frequency** - This setting is used to prevent multiple alarms of the same state from the same device. Duplicate alarms will be ignored if they occur within the specified time period." (4-26) [SYM_P_0081024]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Alarm – Enum – Specifies whether the control should check any of the threshold properties for alarm conditions, and if so, which thresholds to evaluate. Defaults to Disabled. (Disabled (0), Min/Max Thresholds (1), Norm/Alarm Values (2)." (7-5) [SYM_P_0081063] "MaxThreshold – Long – Defines the upper limit for the variable. If the variable exceeds this value, and there is not an outstanding alarm condition, an alarm event will be generated and the control will be displayed in AlarmColor if Alarm=Max/Min Thresholds. If the Trap property is set to True an OpenView Alarm will be sent to the AlarmManager." (7-6) [SYM_P_0081064]
3	The method of claim 1, wherein integrating further comprises invoking countermeasures to a suspected attack.	"**Configuring Alarms** Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following: • Change the device symbol to the new status color • Make an entry in the alarm log • Forward an alarm to another management console • Sound an alarm • Run a program" (4-21) [SYM_P_0081019] "OpenView automatically logs an information alarm for each trap it receives. You can change OpenView's default response to traps to sound an alarm, change color of the map symbol for the device sending the trap, or enter the trap in the alarm log. You can also change the default response to ignore traps from some or all devices, or configure one trap to auto-acknowledge another one when it is received. Each device class (hub type 1, hub type 2, router, server, etc.) can be assigned a different set of default and customized trap responses." (4-11) [SYM_P_0081009]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		"Running Programs OpenView can run an MS-DOS or Windows program when an alarm is generated. You can select what program is run based on the status of the alarm. Information about the alarm can be passed as command line arguments to the program." (4-29) [SYM_P_0081027] "In addition to running a program with a command line string, the alarm system can also pass information to another Windows application using DDE." (4-31) [SYM_P_0081029] "OpenView ships with the paging program *Notify! Connect* from Ex Machina Corporation. This program sends a paging message to a pager when a specified alarm goes off." (4-31) [SYM_P_0081029]
4	The method of claim 1, wherein the plurality of network monitors include an API for encapsulation of monitor functions and integration of third-party tools.	**"SNMP Manager** The Simple Network Management Protocol (SNMP) Version 1.1 is a standard that defines a method of communicating with and controlling network devices. Devices that support the SNMP V.1 standard can be queried for their status and other device information. … OpenView provides an SNMP Management function that can be used to communicate with SNMP devices. The device settings and other device information are available as variables and are defined either in a standard Management Information Base (MIB) file or in a custom MIB file provided by the device manufacturer." (1-7) [SYM_P_0080963] "A proxy agent is a device that acts on behalf of a device that does not have SNMP capabilities. The trap manager uses the Proxy Agent field." (4-2) [SYM_P_0081000] **"Configuring Alarms** Applications monitor the state of network devices and processes and can trigger alarms. The alarms alert network managers of changes in the status of a device or group of devices. When an application detects a change in a device status, it can request OpenView to do one or more of the following:

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		. . . • Run a program" (4-21) [SYM_P_0081019] "The SNMP Version 1 network devices store information about themselves in a Management Information Base (MIB). A MIB contains variables that describe the characteristics and current state of a network device. The SNMP Manager can access this information and control network devices that support SNMP." (5-1) [SYM_P_0081033] "The accessible SNMP variables are listed in the Variables box and may come from various MIBs. An extensive set comes with OpenView. Applications installed into OpenView may have added their own MIBs to the list. You may also use the MIB compiler to add MIBs." (5-3) [SYM_P_0081035] ------------------------------------ "This memo describes the common structures and identification scheme for the definition of management information used in managing TCP/IP-based internets. Included are descriptions of an object information model for network management along with a set of generic types used to describe management information. Formal descriptions of the structure are given using Abstract Syntax Notation One (ASN.1) [1]. This memo is largely concerned with organizational concerns and administrative policy: it neither specifies the objects which are managed, nor the protocols used to manage those objects. These concerns are addressed by two companion memos: one describing the Management Information Base (MIB) [2], and the other describing the Simple Network Management Protocol (SNMP) [3]." (RFC 1155 p. 2) [SYM_P_0501013] "A collection of object types is defined in the MIB. Each such subject type is uniquely named by its OBJECT IDENTIFIER and also has a textual name, which is its OBJECT DESCRIPTOR." (RFC 1155 p. 10) [SYM_P_0501021]
5	The method of claim 1,	"**IP Discovery** uses routers to discover and identify all IP devices in your network." (2-2) [SYM_P_0080966]

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
	wherein the enterprise network is a TCP/IP network.	"This mask should be specific to your local network and also the same as the mask you specified when you installed your TCP/IP protocol stack." (2-4) [SYM_P_0080968] --- "This memo describes the common structures and identification scheme for the definition of management information used in managing TCP/IP-based internets." (RFC 1155 p 2) [SYM_P_0501013]
6	The method of claim 1, wherein the network monitors are deployed at one or more of the following facilities of the enterprise network: {gateways, routers, proxy servers}.	"To start a discovery, you need to know some information about your own network and the networks you want Autodiscovery to search. To run an IP discovery, you must provide the following information: . . . The IP address and community name for your default gateway or router if present." (2-2) [SYM_P_0080966] "Devices in the network are displayed on maps. Devices and subnetworks can be organized into submaps to suit your needs. You can create separate submaps of devices grouped by device function, network function, network organization, or corporate organization. You can use the maps to manage your network from a single display even when the network includes devices from different manufacturers. Programs that manage hubs, routers, servers, and other network devices can run in the background. Changes in network status are displayed on network maps with icons representing devices. Color is used to indicate device status. Submaps allow you to create several views of your network to simplify management. You can add meaningful graphics such as geographic maps and floor plans as backgrounds for your map to provide "real world" visual references for your network." (1-2) [SYM_P_0080958] "The **Component** symbol set contains various network components such as hubs, routers, and multiplexers. OpenView applications can add symbols or delete symbols from the standard set." (3-14) [SYM_P_0080996] --- "Implicit in the SNMP architectural model is a collection of network management stations and network elements. Network management stations execute management applications which monitor and control network elements. Network elements are devices

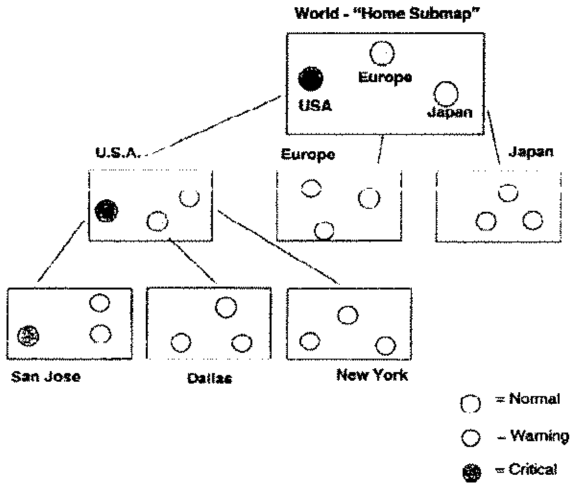
HP OpenView for Windows User Guide
“HP OpenView”

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		such as hosts, gateways, terminal servers, and the like, which have management agents responsible for performing the network management functions requested by the network management stations. The Simple Network Management Protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements.” (RFC 1157 p. 4) [SYM_P_0527111] “Upon receiving a subtree, the enterprise may, for example, define new MIB objects in this subtree. In addition, it is strongly recommended that the enterprise will also register its networking subsystems under this subtree, in order to provide an unambiguous identification mechanism for use in management protocols. For example, if the "Flintstones, Inc." enterprise produced networking subsystems, then they could request a node under the enterprises subtree from the Internet Assigned Numbers Authority. Such a node might be numbered: 1.3.6.1.4.1.42 The "Flintstones, Inc." enterprise might then register their "Fred Router" under the name of: 1.3.6.1.4.1.42.1.1” (RFC 1155 p. 6) [SYM_P_0501017] “See also the Host and Gateway Requirements RFCs for more specific information on the applicability of this standard.” (RFC 1155 p. 1) [SYM_P_0501013] “sysServices OBJECT-TYPE . . . ‘ . . . layer functionality 1 physical (e.g., repeaters) 2 datalink/subnetwork (e.g., bridges) 3 internet (e.g., IP gateways)

HP OpenView for Windows User Guide
"HP OpenView"

'203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		4 end-to-end (e.g., IP hosts) 7 applications (e.g., mail relays) For systems including OSI protocols, layers 5 and 6 may also be counted.'" (RFC 1213 p. 14) [SYM_P_0501155-SYM_P_0501156] "ipForwarding OBJECT-TYPE SYNTAX INTEGER { forwarding(1), -- acting as a gateway not-forwarding(2) -- NOT acting as a gateway }" (RFC 1213 p. 25) [SYM_P_0501165] "Remote network monitoring devices are instruments that exist for the purpose of managing a network. Often these remote probes are stand-alone devices … An organization may employ many of these devices, one per network segment, to manage its internet." (RFC 1271 p. 3) [SYM_P_0501208] -- See Figure 13 in my expert report.
7	The method of claim 1, wherein deploying the network monitors includes placing a plurality of service monitors among multiple domains of the enterprise network.	"Before you create a network map, you need to know the physical layout of your network. If may be a single LAN, several LANs, or a very complex enterprise-wide network. Whenever possible you should break your map into submaps that help you visualize the network organization. You can create submaps for a workgroup, building site, device type, or any other convenient grouping. The same device can be placed on several submaps to provide alternate "views" of the network. … The submap symbol displays the most severe status color for all of the nodes or devices within it. This allows the most severe status information for any device in the network to be propagated up to the home submap. The home submap can then give you an overview of status for the entire network." (3-2) [SYM_P_0080984]

HP OpenView for Windows User Guide
“HP OpenView”

’203 Claim number	Claim Term	HP OpenView (printed publication and public use)
		 World - “Home Submap” USA Europe Japan U.S.A. Europe Japan San Jose Dallas New York ○ = Normal ○ - Warning ● = Critical “Figure 4-2 Map set to propagate alarms up all levels.” “Normally, you would select to propagate up all levels. Then, if your home submap contains a submap symbol for each submap in the next lower level in the map, you can check your network’s overall status from the home submap. If a submap represents several devices, its submap symbol on the home submap will display the most severe device status for the lower submap.” (4-19) [SYM_P_0081017]